ADOA Information Security

AIS Managing Our Information Safeguards

The Attack of the Zombies

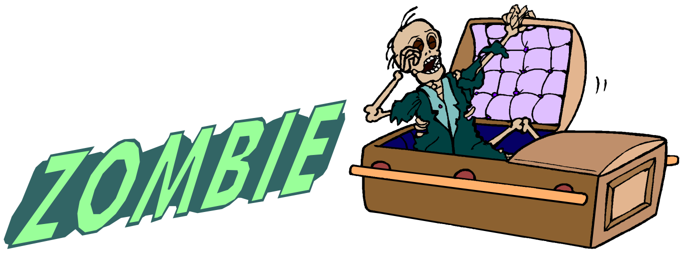
Has Your Computer Been Taken Over by a "ZOMBIE" Virus?

WHO'S RESPONSIBLE?

YOU ARE!

It is your responsibility to watch out for ghosts, werewolves, vampires, demons, witches and even black cats that are in Cyber Space lurking in the dark just waiting for the right moment to turn your computer into a "ZOMBIE".

BEWARE…



Cyber Security Awareness Month

October 2006

ADOA Information Security

AIS Managing Our Information Safeguards

HAUNTING THOUGHT: Is Your PC a Zombie?

Basic content from an article by: Mary Landesman - http://antivirus.about.com/mbiopage.htm

In *The Night of the Living Dead*, zombies sucked brain matter in a frenzied hunger. In the computer world, a Trojan can be used to turn your PC into its own computing matter - turning it into a zombie machine. Once under the control of such an illicit program, the Trojan can be accessed by attackers intent on any number of ominous deeds.

Trojans have the same right on the system as does the logged in user. In other words, if the user can, the Trojan can. This includes deleting or modifying files, installing other software, uninstalling software, or sending sensitive password and login information to a remote attacker.

Computers affected by Trojans can be used to launch attacks against targeted Internet sites. By having thousands of computers accessing the same site at the same moment, the site servers can sometimes become overwhelmed and may no longer be able to process requests. These attacks, referred to as **Distributed Denial of Service or DDoS**, attacks, are fairly common.

CREATING A BOTNET - Just how do Trojans get on the system? Many are sent via email attachment, masquerading as a legitimate piece of software. When the user executes the attachment, the Trojan installs itself to their system. In most cases, there is no indication this has occurred, and the user innocently plays the game before sending it on to the next victim. While email attachments may be the most common, there are dozens of others ruses used. One of the biggest risks, far outweighing that of email attachments, are files downloaded via anonymous P2P filesharing networks.

Regardless of how the infection gets on the system, once installed, the system is under the control of the attacker. Often, the attacker will share the list of zombied systems with others, giving unfettered access to their collection of zombie machines by other ill-intended criminals. Attackers can also often simply scan for compromised machines, which often send a greeting of readiness to listening ears. Collectively, the zombied systems are referred to as a botnet.

These botnets are then used for a variety of criminal purposes – all of which pose serious risk to the infected user as well as the entire Internet community. And while some may not care about the risk to the Internet as a whole, remember that many of today’s threats include keylogging capabilities. Of special interest to the attackers are any personal financial details – which are then used for everything from credit card theft to outright identity theft. In short, it’s not just your computer at risk – it’s your wallet.

While it may be tempting to think it cannot happen to you, think again. Malicious code has evolved far beyond the childish pranks of yesteryear. Today's attackers are serious criminals, in it for the money, and they need as many systems under their control as they can get. If your computer isn't properly protected, it's not a matter of whether it's part of a botnet inasmuch as it's a matter of how long and how bad. While broadband users are the favorite targets, even dial-up users can be unwitting participants. Various studies have demonstrated that any vulnerable system can be compromised within as little as 5 minutes online.

PROTECTING AGAINST TROJANS - PREVENTION is the key. Don't open unanticipated file attachments from unknown sources. If you know the source, double check with them to ensure they intended to send it. Ask them exactly what it is and why you need it. If it is a game or frivilous application, delete it. Save any attachment you have a need to open and scan it with an up-to-date antivirus scanner before you launch it.

FIREWALL your system. Antivirus software is a must, but it is simply not enough. Whether you connect via dial-up, cable, satellite or DSL, and regardless of your ISP, get and use a personal firewall. If you don't have one, the free ZoneAlarm firewall, used properly, can offer excellent protection:

COMPUTE SAFELY. Take control of your email. Avoid opening email attachments received unexpectedly - no matter who appears to have sent it. Remember most worms and Trojan-carrying spam try to spoof the sender's name. Make sure your email client isn't leaving you open to infection. Reading email in plain text offers important security benefits that more than offset the loss of pretty colored fonts.